(12) UK Patent Application (19) GB (11) 2 329 547 (13) A

(43) Date of Printing by UK Office 24.03.1999

(21) Application No 9827621.5

(22) Date of Filing 12.06.1997

(30) Priority Data
(31) 118643 (32) 12.06.1996 (33) IL

(86) International Application Data
PCT/IL97/00191 En 12.06.1997

(87) International Publication Data
WO97/48084 En 18.12.1997

(71) Applicant(s)
Aliroo Ltd
(Incorporated in Israel)
19 Trumpeldor Street, 44442 Kfar Sava, Israel

(72) Inventor(s)
Itzhak Pomerantz
Meir Zorea
Ram Cohen
Tomer Yahav

(51) INT CL[6]
G09C 5/00

(52) UK CL (Edition Q)
H4F FBB FDE

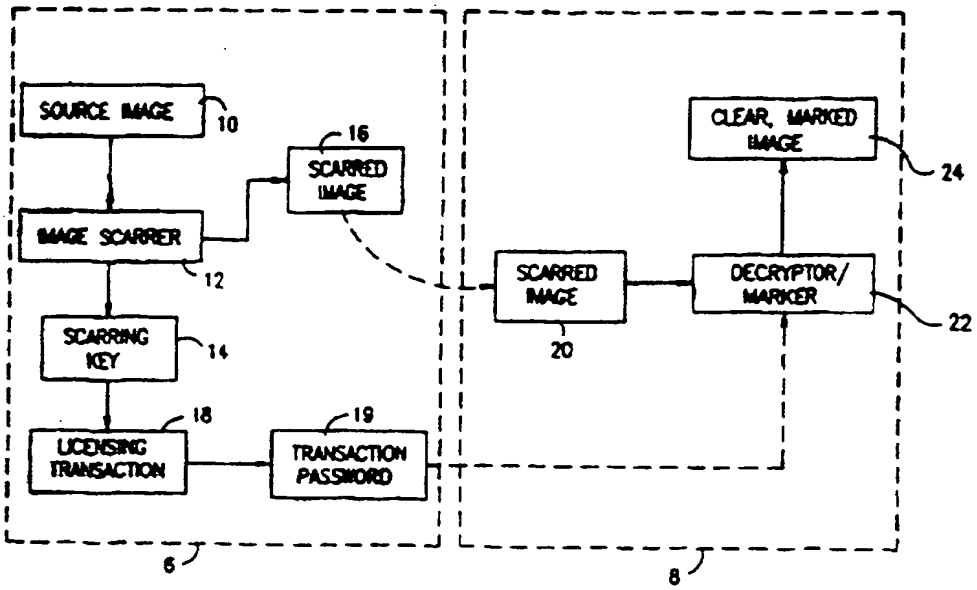
(56) Documents Cited by ISA
EP 0493091 A1 US 5488664 A US 5315098 A
US 4972476 A US 4245213 A US 3914877 A
1979 Conf. on Crime Countermeasures, Lexington, Kentucky, 16-18 May 1979 (W Szepanski); pp.101-109

(58) Field of Search by ISA
U.S. : 382/100, 112, 115, 118, 232; 380/9, 10, 51, 54, 55; 283/17, 72, 73, 85, 113; 235/494

(74) Agent and/or Address for Service
Stephenson Harwood
One, St. Paul's Churchyard, LONDON, EC4M 8SH, United Kingdom

(54) Abstract Title
Security tagging of digital media

(57) A system for protecting digital images provided to a recipient against unauthorized use and transfer including a scarrer (2) for operating on the digital image (10) to cause at least one encrypted scar to appear on the image (16), which other than bearing the scar may be used and manipulated by a recipient and a descarrer (22) operated by a decryption key for removing the at least one encrypted scar from the image.



GB 2 329 547 A

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 5/00

A1

(11) International Publication Number: WO 97/48084

(43) International Publication Date: 18 December 1997 (18.12.97)

(21) International Application Number: PCT/IL97/00191

(22) International Filing Date: 12 June 1997 (12.06.97)

(30) Priority Data:
118643 12 June 1996 (12.06.96) IL

(71) Applicant *(for all designated States except US)*: ALIROO LTD. [IL/IL]; Trumpeldor Street 19, 44442 Kfar Sava (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: POMERANTZ, Itzhak [IL/IL]; Golomb Street 18, 44357 Kfar Sava (IL). ZOREA, Meir [IL/IL]; Harav Herzog Street 33, 76310 Rehovot (IL). COHEN, Ram [IL/IL]; Bartenura Street 13, 62280 Tel Aviv (IL). YAHAV, Tomer [IL/IL]; Yahin Street 4, 52491 Ramat Gan (IL).

(74) Agents: COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

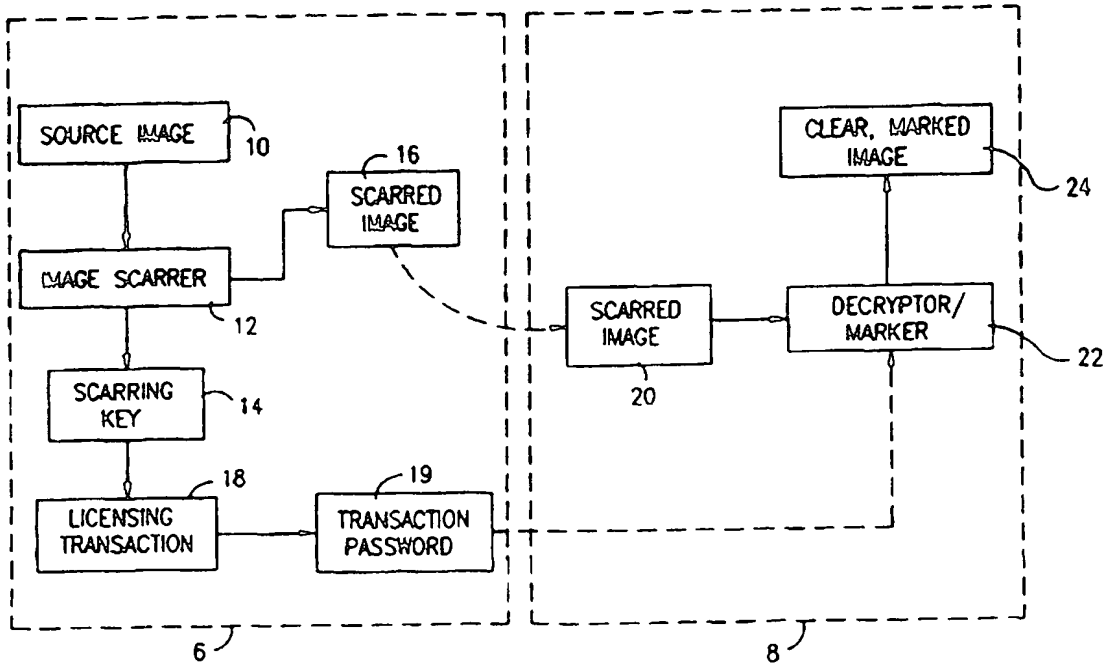
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURITY TAGGING OF DIGITAL MEDIA



(57) Abstract

A system for protecting digital images provided to a recipient against unauthorized use and transfer including a scarrer (2) for operating on the digital image (10) to cause at least one encrypted scar to appear on the image (16), which other than bearing the scar may be used and manipulated by a recipient and a descarrer (22) operated by a decryption key for removing the at least one encrypted scar from the image.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SECURITY TAGGING OF DIGITAL MEDIA

The present invention relates to digital image processing generally and more particularly to security tagging of digital media.

Commercial licensing of images such as photographs is well known. Generally, the owner of rights in an image provides the image to a potential licensee for evaluation. If the potential licensee wishes to use the image, he enters into a license agreement with the rights owner.

Unfortunately, an unscrupulous potential licensee may make unlicensed use of the image, or even worse, pass it on to others, without authorization of the rights owner. The essential difficulty lies in the fact that provision of the image to a potential licensee in effect constitutes full delivery of that image, such that the image ceases to be under the control of the rights owner.

Various proposals have been made to overcome this difficulty. Some of these proposals are reviewed in an article entitled "Handcuff Digital Thieves" by Philip Chudy, In Byte Magazine, International Edition, April, 1996, page 40.

The prior art proposals may be divided into two categories:

preventative measures which render the image unusable by the prospective licensee prior to payment of licensing fees. Two common methods of this type are to encrypt the data file and to deny access to the file location until licensing fees are paid.

fingerprinting methods whereby the image is invisibly marked to indicate the ownership of the rights. The fingerprint can be relied upon in legal proceedings to prove the ownership rights in the image.

Commercial products for implementing both types of proposals are available from HighWater FBI Ltd. 2-6 St. George's Business Park, Alstone Lane, Cheltenham, Gloucestershire, GL51 8HF, United Kingdom; Fraunhofer Institute for Computer Graphics, Wilhelminestr. 7, 64283 Darmstadt, Germany and Digimarc Corporation 1850 NW 113th Avenue, Portland, Oregon 97229, USA.

Unfortunately both types of proposals have serious limitations. The preventative methods do not allow the prospective licensee to evaluate and experiment

with the actual image prior to licensing it. The fingerprinting methods do not identify the unscrupulous potential licensee who has illegally used or transferred the image.

The present invention seeks to overcome the limitations of the prior art methods and apparatus and to provide apparatus and a method of allowing a potential licensee to evaluate and experiment with an image prior to licensing it, but without allowing him to make commercial use of it or transfer it to another for production work.

In this specification and claims the terms "scrambling" and "encrypting", and the terms "descrambling" and "decrypting" are respectively synonymous.

There is thus provided in accordance with a preferred embodiment of the present invention apparatus for protecting digital images provided to a recipient against unauthorized use and transfer including scarring apparatus for operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient, and descarring apparatus operated by encryption key for removing the at least one encrypted scar from the image.

In accordance with a preferred embodiment of the present invention, the descarring apparatus is also operative to implant an invisible transaction record in the image which identifies the recipient and preferably also the licensing transaction.

Further in accordance with a preferred embodiment of the present embodiment the encrypted scar comprises a plurality of gixels each including a plurality of pixels and wherein the pixels are scrambled within their respective gixel.

Still further in accordance with a preferred embodiment of the present invention the encrypted scar includes a plurality of pixels, each pixel including color information, and wherein at least some of the plurality of pixels have scrambled color information.

In accordance with a preferred embodiment of the present invention, the encrypted scar includes a plurality of scar gixels which are scrambled.

Preferably, the encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

There is also provided in accordance with a preferred embodiment of the present invention apparatus for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

a scarrer for operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient.

There is additionally provided in accordance with a preferred embodiment of the present invention descarring apparatus operable to manipulate digital images bearing at least one encrypted scar, which other than bearing the scar may be used and manipulated by a recipient, the apparatus including a descarrer operated by an decryption key for removing the at least one encrypted scar from the image.

In accordance with a preferred embodiment of the present invention, the descarrer is inoperative for removing the at least one encrypted scar from the image without also embedding an invisible marker in the image, the marker preferably being a transaction record which may identify the recipient and/or also the licensing transaction.

In this specification the term "recipient" includes the person who descarrs the image, and this may be the same person as the one who scarred the image in the first place. It also includes any person who receives the image and does not descarr it for any reason.

There is additionally provided in accordance with a preferred embodiment of the present invention a method for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient; and

using a decryption key, removing the at least one encrypted scar from the image.

Further in accordance with a preferred embodiment of the present invention the encrypted scar comprises a plurality of gixels each including a plurality of pixels and wherein the pixels are scrambled within their respective gixel.

Still further in accordance with a preferred embodiment of the present invention the encrypted scar includes a plurality of pixels, each pixel including color information, and wherein at least some of the plurality of pixels have scrambled color information.

The method also preferably includes the step of at the time of removing the scar also implanting an invisible marker in the image, the marker perhaps being a transaction record which identifies the recipient and/or the licensing transaction.

Preferably, the step of removing the encrypted scar from the image cannot be carried out without also embedding an invisible marker in the image, which record may identify the recipient and preferably also the licensing transaction.

There is additionally provided in accordance with a preferred embodiment of the present invention a method for protecting digital images provided to a recipient against unauthorized use and transfer including operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient.

There is further provided in accordance with a preferred embodiment of the present invention a method of operating on digital images bearing at least one encrypted scar, which other than bearing the scar may be used and manipulated by a recipient, the method comprising using an decryption key to remove the at least one encrypted scar from the image.

Preferably, at the time of removing the scar, an invisible transaction record must be implanted in the descarred image, which record may identify the recipient and/or the licensing transaction.

Preferably, the encrypted scar includes a plurality of gixels each comprising a plurality of pixels, comprising the step of scrambling said pixels within their respective gixel.

Preferably the encrypted scar includes a plurality of pixels, each pixel comprising color information, said method further comprising the step of scrambling the color information of at least some of said plurality of pixels.

It is noted that the present invention finds application inter alia in remote transmission of images for the purpose of licensing as well as in providing security in local archives.

The present invention will be understood and appreciated more fully from the following detailed description, given purely by way of example, taken in conjunction with the drawings in which:

Fig. 1 is a generalized functional block diagram of a system for protecting digital images provided to a recipient against unauthorized use and transfer, constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 2A and 2B are simplified block diagram illustrations of scarring and descarring functionalities respectively carried out in accordance with a preferred embodiment of the present invention;

Figures 3A to 3E are illustrations of a typical image operated on by the system of Fig. 1 in unscarred and scarred states;

Appendix A is a listing of the source code of a scarring program; and

Appendix B is a listing of the source code of a password-splitting program.

Reference is now made to Fig. 1, which is a generalized functional block diagram of a system, comprising units 6 and 8, constructed and operative in accordance with a preferred embodiment of the present invention, for protecting digital images provided to a recipient against unauthorized use and transfer. A source image 10, such as, for example, the image appearing in Fig. 3A is supplied to an image scarrer 12, which employs an encryption key, here termed a scarring key 14 to encrypt one or more user definable, relatively small, but important portions of the source image to produce a scarred image 16 as seen in Fig. 3B. The scarred image of Fig. 3B has one or more scars 15, which are preferably scrambled portions of the image which contain all of the image information required to construct the complete source image, which information is disordered in accordance with the scarring key 14.

The scar may bear some alphanumeric information by reversing the color of some gixels in the encrypted image. This information can typically serve as a key clue. Upon decryption, the color-reversed pixels or gixels can easily be restored through color

correlation with their local environment. This is particularly helpful in archive security applications where various keys may be employed and may be forgotten by the user.

The source image is typically provided to the scarrer 12 in a conventional bit map format such as, for example, BMP, GIF or JPEG. The image scarrer may operate according to any suitable encryption program, such as, for example, the program whose listing is appended hereto as Appendix A.

The resulting scarred image, as exemplified by Fig. 2B may be transmitted to a recipient, such as a potential licensee, at a remote location by using conventional communications and handled by the recipient like any other digital image for purposes of experimentation and evaluation.

Should the recipient decide to obtain rights to use the image 18, the rights owner may generate a transaction password 19 upon receipt of payment or of an acceptable order. In accordance with a preferred embodiment of the present invention, the transaction password 19 includes not only the scarring key 14 but also a transaction identifier which can be used to identify the specific transaction and the recipient. Upon completion of the rights transaction, the transaction password 19 is transferred to the recipient using conventional communications.

The recipient may employ a program, the listing of the source code of which appears in Appendix B, to receive the transaction password 19 and extract the scarring key 14 and the transaction identifier. A document marker 22, which may employ the fingerprinting software available from Digimarc Corporation, Portland Oregon, preferably carries out the following two functions and is prevented from carrying out the first without carrying out the second:

1. Descrambling of the scars using the scarring key 14 to produce an unscarred image.

2. Embedding an invisible to the eye but electronically detectable transaction identifier which identifies the recipient and preferably also the licensing transaction and preferably also identifies the rights owner and contains a transaction number.

In summary it is appreciated that the document marker 22 thus operates on the received scarred image 20 to produce an unscarred image 24, which bears an invisible transaction record identifying at least the recipient and the rights owner. This

transaction record is retained in the image even if it is transferred onward to further recipients in an unauthorized manner and cannot normally be erased by an unscrupulous recipient. This enables all future uses of the image to be traced back to the recipient.

It is particularly preferred that the image cannot be unscarred without the invisible transaction record being embodied in the image.

Reference is now made to Figs. 2A and 2B, which are simplified block diagram illustrations of scarring and descarring functionalities respectively carried out in accordance with a preferred embodiment of the present invention.

As illustrated in Fig. 2A, the scarring process includes the steps of opening a source image in a scarring tool, such as the software set forth in Appendix A, and selecting an encryption key for use as the scarring key 14 (Fig. 1) for use in scarring.

The scarring process is carried out by the user, who would typically be the one responsible for protecting the rights of the rights owner in the image, and, having selected an encryption key he would then proceed to select one or more encryption modes. Three encryption modes are typically provided and these include:

1. shuffling gixels, that is rectangles of one or more pixels - see below- within the scar area,
2. shuffling pixels within a gixel, and
3. modifying the color values within a pixel.

The next step in the process comprises defining a scar area within the image. This step may be carried out automatically by a program that places random scars in the image. Alternatively it may be carried out manually by a person having an understanding of the commercial usefulness of the image so as to select a scar area which does not prevent full evaluation of the image by a potential licensee, but nevertheless prevents unauthorized use of the image until the scar is removed.

A size of scar gixel is preferably selected. The scar tile may correspond to a gixel, where a gixel is a contiguous rectangle of pixels that can be moved around the image preserving its internal structure, as described in applicant/assignee's U.S. Patent 5,491,563, the disclosure of which is hereby incorporated by reference. A gixel may be as small as a single pixel. Reference is also made in this connection to the following

patent applications of applicant/assignee, the disclosures of which are also incorporated herein by reference:

Israel Patent Applications 106567, 120231 & 109591, U.S. Patent Application Serial No. 08/131,326.

Israel Patent Application 120231, which is not prior art to the present application, describes how the present invention may be applied to a sound file.

Israel Patent Application 109591 discloses inter alia a scrambling transformation that can be applied to gixels. In this transformation the relative position of the gixels is changed but within each gixel the pixels are unchanged. This document also discloses considerations involved in choosing the most appropriate size of gixel. Details of the descrambling process are also discussed and the reader is referred to pages 34-68 of this document.

It is noted that some graphic formats have a natural gixel size that is handled by the format as a single entity. For example JPEG has a natural gixel size of 8 x 8 pixels. In such cases the scarring tool may be adjusted to this preferred gixel size.

If mode 1. above has been selected then the scar is scrambled by shuffling gixels around the scar according to the selected scarring key 14. An advantage of gixel shuffling is that the image is better disguised than in the other methods, and another advantage is that it is fast relative to pixel shuffling.

If mode 2. is selected then pixels are shuffled around the gixel. An advantage of moving pixels rather than gixels is that the general shape of the image is preserved within the scar. However the quality is not good enough for commercial use of the image.

Additionally or alternatively whole gixels may be shuffled about without changing the gixel itself. An advantage in gixel shuffling is that it is faster than pixel shuffling, and gixel shuffling also provides a better concealment of the image.

If mode 3. is selected then the color values within the pixel are randomized. The color information within a pixel is generally represented by three numerical values representing respective strengths of red, green and blue (R, G, B). In other systems four values (C, M, Y, K) can be used. In some images a single value may be used, simply to represent gray levels and it is also known to have a single binary value

to represent black and white (B & W). The advantage of randomizing the color values is that it produces an easy calculation, the disadvantage is that it produces an ugly scar.

It is particularly advantageous to randomize the color values in combination with one or both of the shuffling methods as the combination increases the cryptographic strength of the scar.

Additional scars may be added as determined by the user and the scarred image is then delivered to the potential licensee.

Referring now to Fig. 2B, it is seen that the potential licensee opens the scarred image in a conventional graphics editor, such as PHOTOSHOP R or CORELDRAW R and, having experimented with and evaluated the scarred image to his satisfaction, initiates a licensing transaction. Having paid the licensing fee or otherwise made the necessary financial arrangements with the owner of the rights, he receives a licensing password, which corresponds to the transaction password 19 (Fig. 1), from the rights owner.

The licensee employs the descarring tool, preferably provided to the licensee for free by the owner of the rights, uses it to extract both the descarring key and transaction identifier from the licensing password, and applies them to the scarred image. Preferably this is done using software which prevents him from employing the descarring key without applying the transaction identifier as an embedded invisible label in the resulting descarred image. To this end, the extraction of the descarring key is carried out internally in a manner which does not allow the recipient to tamper with the results.

The descarred, transaction identified image may then be stored for authorized use. Should the image be subsequently transferred for unauthorized use, digital examination of the unauthorized image will disclose the transaction identification embedded therein, including identification of the recipient who transferred the image without authority or made an unauthorized use thereof.

Figure 3A shows a computerized image to which the system of figure 1 may be applied. Figure 3B shows the image with a scar that has been created by gixel shuffling. It will be apparent that the shape of the image is effectively disguised. Figure 3C shows the image with a scar formed by shuffling pixels within a gixel. It will be seen that the general shape of the image is preserved although the quality is reduced

sufficiently to prevent commercial use of the image. Figure 3D shows a scar formed by shuffling both pixels and gixels, and figure 3E shows a scar formed by randomizing the colors of a pixel.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims which follow the attached appendices:

Appendix A
Source code of a scarring program

```
Variables:
WORD m_BitCount - No. of bits per pixel in image
WORD m_Width    - Width of DIB image in pixels
WORD m_Height   - Height of DIB image in pixels
BYTE HUGE *m_lpDibBits - Memory location of DIB image (points to the
                         beginning of the LAST line of the image)
char [] m_Password - Holds the password with which to scramble/descramble
BOOL bDescramble- Scrambling or Descrambling flag
RECT rect       - The rectangle area to be scrambled\descrambled
WORD TILE_X     - Width of a single tile in pixels (in multiples of 8)
WORD TILE_Y     - Height of a single tile in pixels

BOOL Scramble(BOOL bDescramble,RECT &rect)
{
        // calculate how many tiles in rect
        UINT width = rect.right - rect.left;
        UINT height = rect.bottom - rect.top;
        UINT tiles_x = width / TILE_X;
        UINT tiles_y = height / TILE_Y;
        DWORD tot_tiles = (DWORD)tiles_x * tiles_y;

        //-allocate memory to hold permutation
        HGLOBAL   hpermute = GlobalAlloc(GPTR,tot_tiles *
sizeof(DWORD));
        DWORD     huge *permute = (DWORD huge
*)GlobalLock(hpermute);

        DWORD     k;
        WORD i,j,dest_tile_x,dest_tile_y;
        WORD      ii;
        WORD bpp,bpp2;

        // create permutation
        MakePermutation(permute,tot_tiles,bDescramble);

        // Now, scramble the bitmap

        // allocate memory for temporary rectangle image
        bpp = m_BitCount / 8;
        if (bpp < 1) bpp = 1;
        bpp2 = 0;
        if (m_BitCount == 4) bpp2 = 1;
        else if (m_BitCount == 2) bpp2 = 2;
        else if (m_BitCount == 1) bpp2 = 3;
```

```
        DWORD     dwSize = ((DWORD)height * width * bpp) >> bpp2;
        HGLOBAL   hMem = GlobalAlloc(GPTR,dwSize);
        BYTE huge *lpMem = (BYTE huge *)GlobalLock(hMem);
        DWORD     DibAddLine = ((((DWORD)m_Width * m_BitCount + 31) /
32) * 32) / 8;
        DWORD     ImgAddLine = ((DWORD)width * bpp) >> bpp2;

        BYTE huge *toPtr;
        BYTE huge *fromPtr;

        // copy with permutation from DIB to temporary rectangle memory
        for(i=0;i<tiles_y;i++) {
                for(j=0;j<tiles_x;j++) {
                        k = permute[(DWORD)i * tiles_x + j];
                        dest_tile_y = (WORD)(k / tiles_x);
                        dest_tile_x = (WORD)(k % tiles_x);

                        toPtr = lpMem + (height - 1 - i * TILE_Y) * ImgAddLine +
                                        ((j * bpp * TILE_X) >> bpp2);
                        fromPtr = m_lpDibBits + (m_Height - 1 - (rect.top +
dest_tile_y * TILE_Y)) * DibAddLine + (((rect.left + dest_tile_x * TILE_X) *
bpp) >> bpp2);

                        // Copy the tile
                        for(ii=0;ii<TILE_Y;ii++) {
                                WORD jj;
                                for(jj=0;jj<((bpp*TILE_X) >> bpp2);jj++)
                                        *(toPtr++) = *(fromPtr++);

                                toPtr -= (ImgAddLine + ((bpp*TILE_X) >> bpp2));
                                fromPtr -= (DibAddLine + ((bpp*TILE_X) >>
bpp2));
                        }
                }
        }

        // now, copy entire rectangle back to the DIB

        for(i=0;i<height;i++) {
                fromPtr = lpMem + i * ImgAddLine;
                toPtr = m_lpDibBits + (m_Height - rect.bottom + i) * DibAddLine
+
                                ((rect.left * bpp) >> bpp2);
                _fmemcpy(toPtr,fromPtr,(width * bpp) >> bpp2);
        }

        // free allocated memory
        GlobalUnlock(hMem);
        GlobalFree(hMem);
```

```
        GlobalUnlock(hpermute);
        GlobalFree(hpermute);

        return TRUE;
}

void MakePermutation(DWORD __huge *permute,DWORD num,BOOL
bRev)
{
        DWORD i,k,j;
        WORD        seed;

        seed = 1;
        for(i=0;i<strlen(m_Password);i++)
                seed *= m_Password[i];

        srand(&seed);

        for(i=0;i<num;i++) permute[i] = i;

        for(i=0;i<num-1;i++) {
                j = (((WORD)rand() << 8) | rand()) & 0x7FFF;
                j = i + j % (num - i - 1);
                k = permute[i];
                permute[i] = permute[j];
                permute[j] = k;
        }

        // when descrambling need to create an inverse of the permutation
        if (bRev) {
                HGLOBAL    hper2 = GlobalAlloc(GPTR,num *
sizeof(DWORD));
                DWORD      huge *per2 = (DWORD huge *)GlobalLock(hper2);
                for(i=0;i<num;i++) per2[permute[i]] = i;
                for(i=0;i<num;i++) permute[i] = per2[i];
                GlobalUnlock(hper2);
                GlobalFree(hper2);
        }
}
```

Appendix B

Source code of a password-splitting program

```
void Split(DWORD dwNum)
{
        DWORD       dwPassword;
        DWORD       dwSerial;
        int         i;

        dwPassword = dwSerial = 0;

        for(i=0;i<16;i++) {
                dwPassword <<= 1;
                if (dwNum & 1) dwPassword |= 1;
                dwNum >>=1;

                dwSerial <<=1;
                if (dwNum & 1) dwSerial |= 1;
                dwNum >>= 1;
        }

        printf("The password is: %lu\n",dwPassword);
        printf("The serial no. is: %lu\n",dwSerial);
}
```

CLAIMS

1. A system for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

a scarrer for operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient; and

a descarrer operated by a decryption key for removing the at least one encrypted scar from the image.

2. A system according to claim 1 and wherein the descarrer is also operative to implant an invisible marker in the image.

3. A system according to claim 1 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

4. A system according to claim 1 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

5. A system according to claim 2 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

6. A system according to claim 2 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

7. A system according to claim 2 and wherein said descarrer is inoperative for removing the at least one encrypted scar from the image without also embedding an invisible marker in the image.

8. Apparatus for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

a scarrer for operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient.

9. Apparatus according to claim 8 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

10. A system according to claim 8 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

11. Descarring apparatus for use with digital images bearing at least one encrypted scar, which other than bearing the scar may be used and manipulated by a recipient, and including:

a descarrer operated by an encryption key for removing the at least one encrypted scar from the image.

12. Descarring apparatus according to claim 11 and wherein said descarrer is operative to implant an invisible marker in the descarred image.

13. Descarring apparatus according to claim 11 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

14. Descarring apparatus according to claim 11 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

15. Descarring apparatus according to claim 11 and wherein said descarrer is inoperative for removing the at least one encrypted scar from the image without also embedding an invisible marker in the image.

16. A method for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient; and

using a decryption key, removing the at least one encrypted scar from the image.

17. A method according to claim 16 and also comprising the step of implanting an invisible transaction record in the image at the time of removing the scar, which record identifies the recipient.

18. A method according to claim 16 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

19. A method according to claim 16 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

20. A method according to claim 17 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

21. A method according to claim 17 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

22. A method according to claim 17 and wherein said step of removing said encrypted scar from the image cannot be carried out without also embedding an invisible marker in the image.

23. A method for protecting digital images provided to a recipient against unauthorized use and transfer comprising:

operating on the digital image to cause at least one encrypted scar to appear on the image, which other than bearing the scar may be used and manipulated by a recipient.

24. A method according to claim 23 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

25. A method according to claim 23 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

26. A method for use with digital images bearing at least one encrypted scar, which other than bearing the scar may be used and manipulated by a recipient, and including:

using a decryption key, removing the at least one encrypted scar from the image.

27. A method according to claim 26 and wherein at the time of removing the scar, an invisible marker is implanted in the descarred image.

28. A method according to claim 26 and wherein said at least one encrypted scar comprises a plurality of scar gixels which are scrambled.

29. A method according to claim 26 and wherein said encrypted scar contains substantially all of the image information needed to reconstruct the area of the digital image underlying the scar, other than the decryption key.

30. A method according to claim 27 and wherein said step of removing the at least one encrypted scar from the image is prevented from being carried out without also embedding an invisible marker in the image.

31. A system according to claim 2 wherein said encrypted scar comprises a plurality of gixels each comprising a plurality of pixels and wherein said pixels are scrambled within their respective gixel.

32. A system according to claim 2 wherein said encrypted scar includes a plurality of pixels, each pixel comprising color information, and wherein at least some of said plurality of pixels have scrambled color information.

33. A method according to claim 16, wherein said encrypted scar comprises a plurality of gixels each comprising a plurality of pixels, comprising the step of scrambling said pixels within their respective gixel.

34. A method according to claim 16 wherein said encrypted scar comprises a plurality of pixels, each pixel comprising color information, said method further comprising the step of scrambling the color information of at least some of said plurality of pixels.

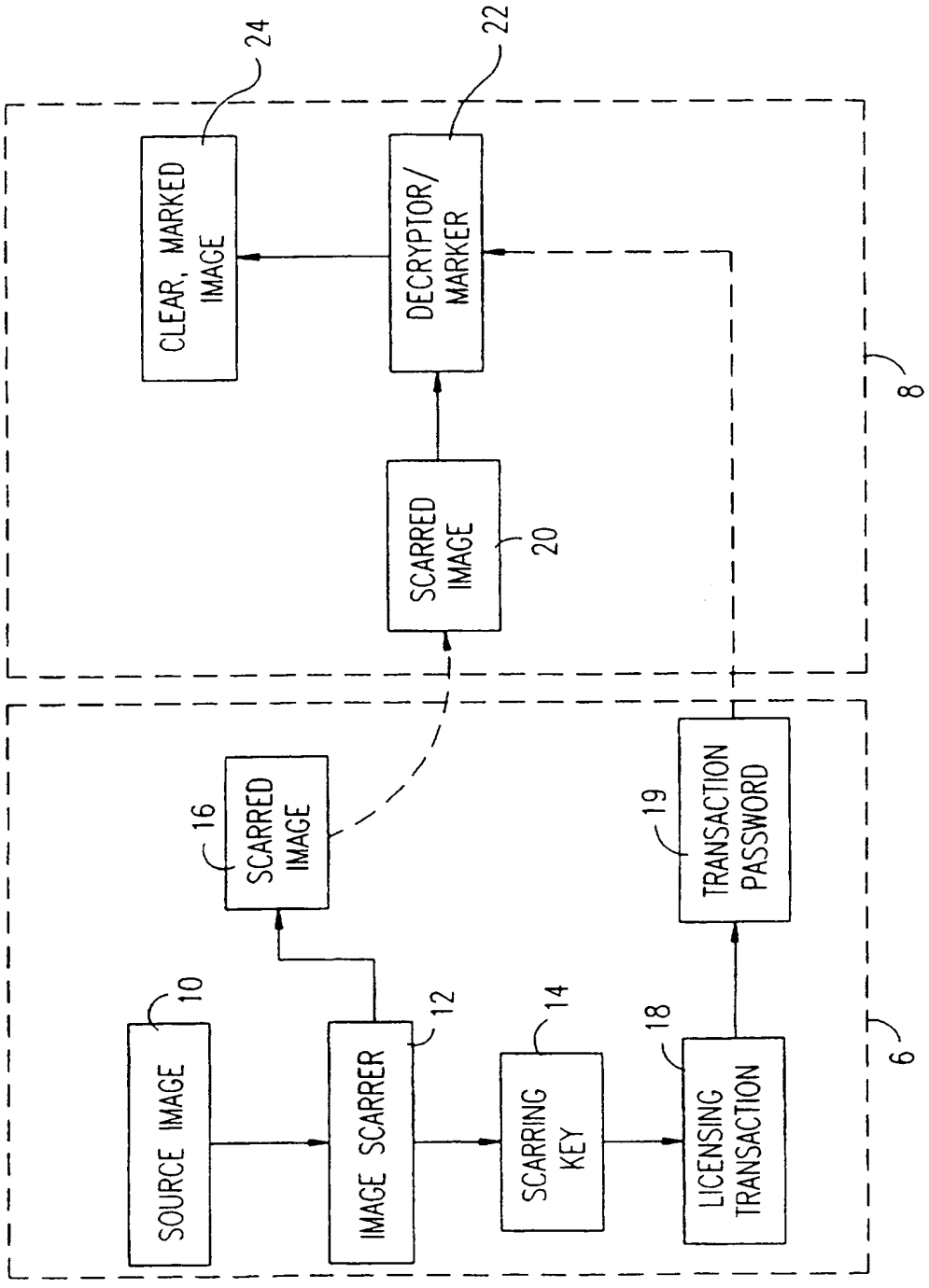

24
22
CLEAR, MARKED IMAGE
DECRYPTOR/ MARKER
8
SCARRED IMAGE
20
16
SCARRED IMAGE
19
TRANSACTION PASSWORD
10
12
14
18
SOURCE IMAGE
IMAGE SCARRER
SCARRING KEY
LICENSING TRANSACTION
6

FIG. 1

FIG. 2A

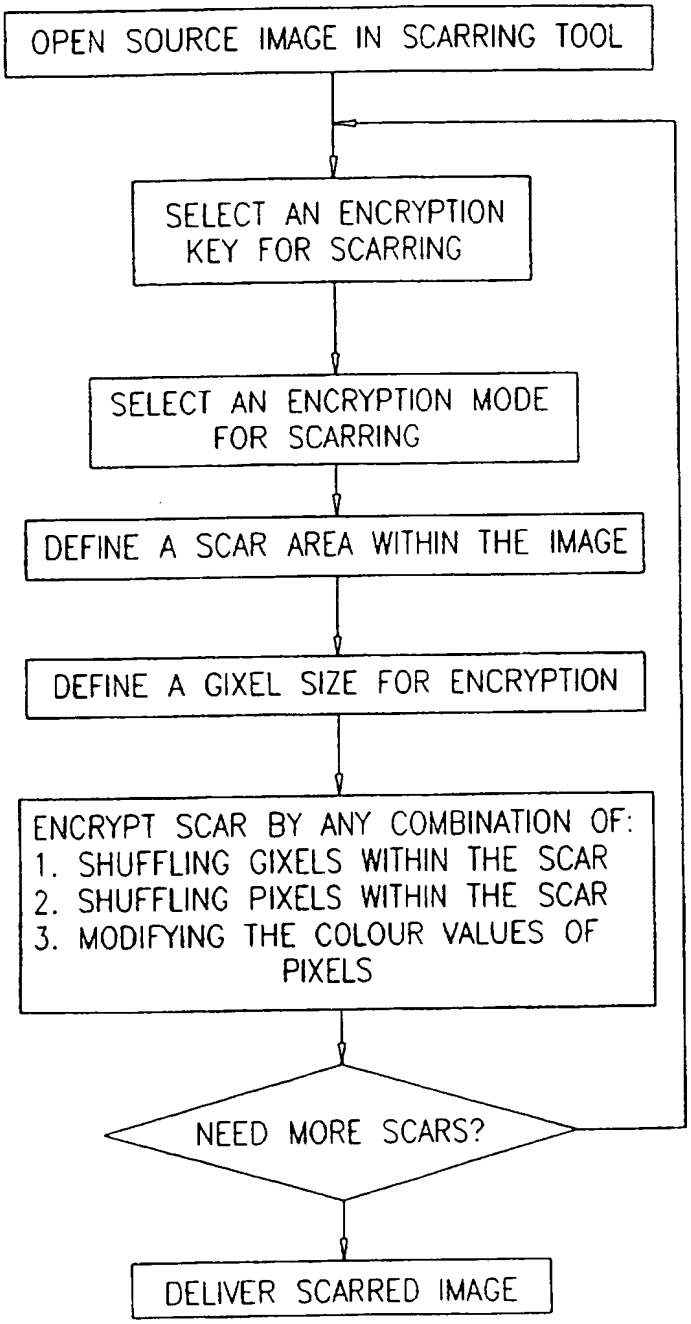

OPEN SOURCE IMAGE IN SCARRING TOOL
SELECT AN ENCRYPTION KEY FOR SCARRING
SELECT AN ENCRYPTION MODE FOR SCARRING
DEFINE A SCAR AREA WITHIN THE IMAGE
DEFINE A GIXEL SIZE FOR ENCRYPTION
ENCRYPT SCAR BY ANY COMBINATION OF:
1. SHUFFLING GIXELS WITHIN THE SCAR
2. SHUFFLING PIXELS WITHIN THE SCAR
3. MODIFYING THE COLOUR VALUES OF PIXELS
NEED MORE SCARS?
DELIVER SCARRED IMAGE

FIG. 2B

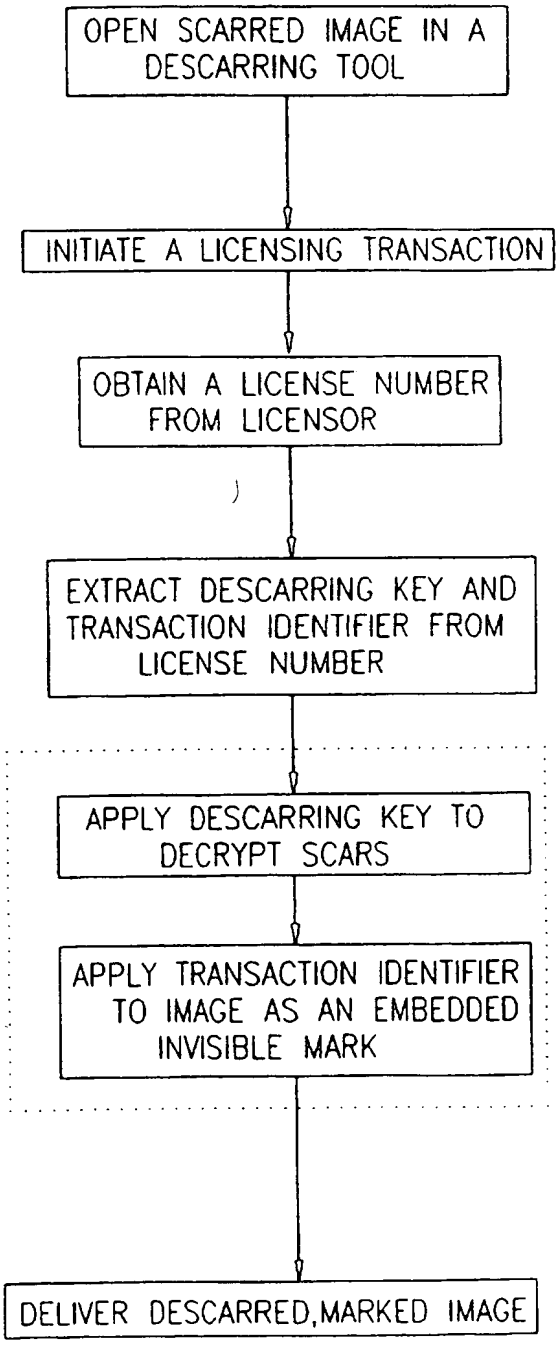
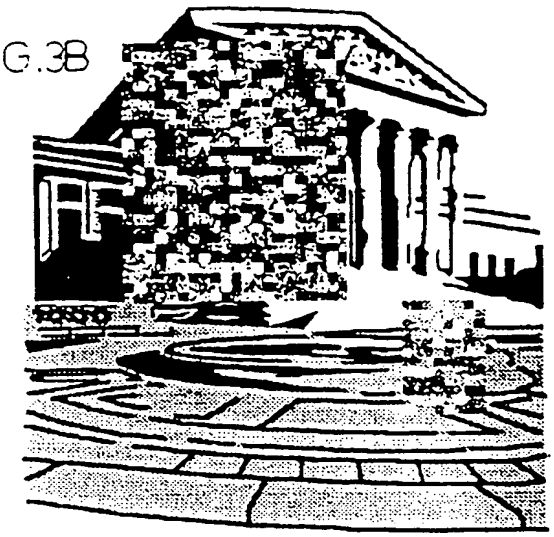

OPEN SCARRED IMAGE IN A DESCARRING TOOL
INITIATE A LICENSING TRANSACTION
OBTAIN A LICENSE NUMBER FROM LICENSOR
EXTRACT DESCARRING KEY AND TRANSACTION IDENTIFIER FROM LICENSE NUMBER
APPLY DESCARRING KEY TO DECRYPT SCARS
APPLY TRANSACTION IDENTIFIER TO IMAGE AS AN EMBEDDED INVISIBLE MARK
DELIVER DESCARRED,MARKED IMAGE

FIG.3A

FIG.3B



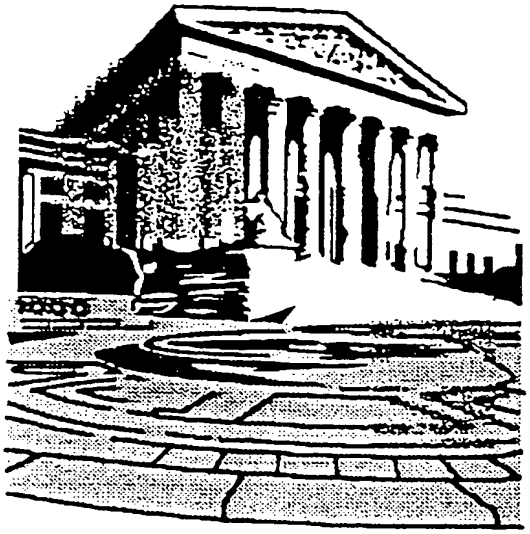


FIG. 3C

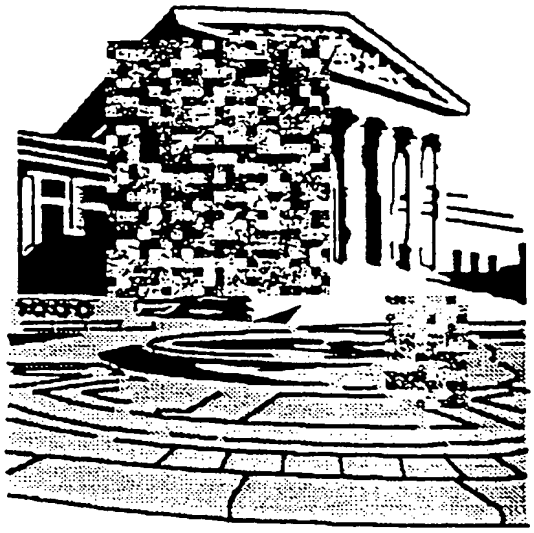
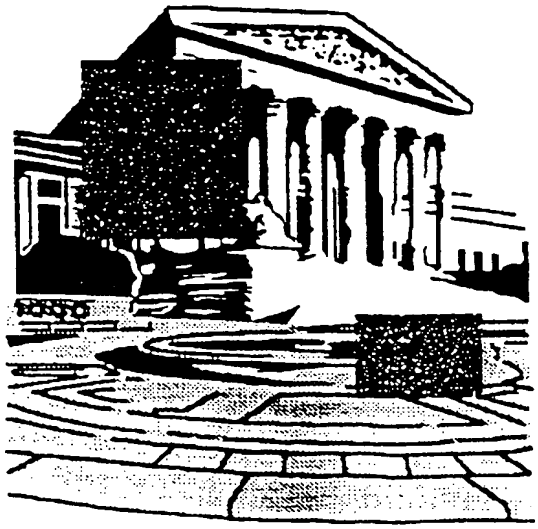


FIG. 3D

FIG. 3E



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL97/00191

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G09C 5/00
US CL :382/100; 380/54

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 382/100, 112, 115, 118, 232; 380/9, 10, 51, 54, 55; 283/17, 72, 73, 85, 113; 235/494

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 4,972,476 A (NATHANS) 20 November 1990, see the Abstract, Figure 1, column 4, line 5 through column 5, line 18.	1, 3-4, 8-11, 13-14, 16, 18-19, 23-26, 28-29, 33-34 ---------- 2, 5-7, 12, 15, 17, 20-22, 27, 30-32
Y	US 5,315,098 A (TOW) 24 May 1994, see the Abstract, column 4, line 22 through column 5, line 9.	2, 5-7, 12, 15, 17, 20-22, 27, 30-32

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
22 OCTOBER 1997

Date of mailing of the international search report
14 NOV 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
ANDREW W. JOHNS
Telephone No. (703) 305-4788

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL97/00191

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 493 091 A1 (TOW) 01 July 1992, see the Abstract, column 2, lines 13-42, column 3, lines 29-58.	2, 5-7, 12, 15, 17, 20-22, 27, 30-32
A	US 5,488,664 A (SHAMIR) 30 January 1996, see the entire document	1-34
A	US 4,245,213 A (KRIGER) 13 January 1981, see the entire document	1-34
A	US 3,914,877 A (HINES) 28 October 1975, see the entire document.	1-34
A	SZEPANSKI, W., A Signal Theoretic Method for Creating Forgery-Proof Documents for Automatic Verification, 1979 Conf. on Crime Countermeasures, Lexington, Kentucky, 16-18 May 1979, pp. 101-109.	1-34